CLAIMS:

1. A method comprising:

receiving input from a remote user of a client device that identifies computer evidence to acquire from a target computing device;

acquiring the computer evidence from the target computing device with a forensic device coupled to the target computing device via a communication link;

storing the computer evidence on the forensic device; and

presenting a user interface for the forensic device through which the remote user views and analyzes the computer evidence acquired from the target computing device.

2. The method of claim 1, wherein presenting the user interface for the forensic device through which the remote user views and analyzes the computer evidence acquired from the target computing device comprises presenting the user interface for the forensic device through which the remote user views and analyzes the computer evidence acquired from the target computing device on-line.

3. The method of claim 1, further comprising acquiring additional computer evidence while the remote user views and analyzes the previously acquired computer evidence.

4. The method of claim 1, wherein acquiring the computer evidence from the target computing device comprises acquiring the computer evidence from the target computing device while the target computing device is active.

5. The method of claim 1, further comprising receiving input from the remote user instructing the forensic device to analyze the computer evidence.

6. The method of claim 1, wherein acquiring the computer evidence from the target computing device comprises acquiring state information from the target computing device.

7. The method of claim 1, wherein acquiring the computer evidence from the target computing device comprises acquiring the computer evidence from the target computing device without pre-loading acquisition software on the target computing device prior to acquiring the computer evidence.

8. The method of claim 1, wherein receiving input from the remote user that identifies computer evidence to acquire comprises receiving input from the remote user that identifies at least one acquisition operation to perform, and further wherein acquiring the computer evidence from the target computing device comprises performing the acquisition operation to acquire the computer evidence.

9. The method of claim 8, wherein performing the acquisition operation comprises communicating commands associated with the acquisition operation to the target computing device to acquire corresponding computer evidence.

10. The method of claim 9, further comprising:

automatically selecting at least one of a plurality of access methods via which to perform the acquisition operation based on the target computing device and the type of computer evidence to acquire; and

communicating commands associated with the acquisition operation to the target computing device via the selected acquisition methods.

11. The method of claim 10, wherein the access methods include at least one of Windows Management Instrumentation (WMI), Server Message Block (SMB), Secure Shell (SSH), Remote Shell (RSH), Network File System (NFS), Apple Filing Protocol (AFP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP).

12. The method of claim 8, wherein the remote user identifies a plurality of the acquisition operations to perform, and wherein acquiring the evidence comprises performing the acquisition operations in an order that reduces the impact on other data stored on the target computing device.

13. The method of claim 12, further comprising performing a subset of the acquisition operations to acquire at least one of an log file and communication statistics prior to performing the other acquisition operations.

14. The method of claim 13, further comprising performing the acquisition operation to acquire the communication statistics after performing the acquisition operation to acquire the log file.

15. The method of claim 13, further comprising performing the acquisition operation to acquire the log file after performing the acquisition operation to acquire the communication statistics.

16. The method of claim 13, further comprising performing an acquisition operation to acquire general system information from the target computing device after performing the subset of the acquisition operations to acquire the at least one of the log file and communication statistics prior to any other acquisition operations.

17. The method of claim 13, wherein the log file comprises one of a system event log, an application event log, and a security event log, web server log file, Unix SYSLOG file, a mail log file, an accounting log file, and a router flow log file.

18. The method of claim 13, wherein the communications statistics comprises one of Ethernet statistics and network protocol statistics.

19. The method of claim 13, further comprising determining an order in which to perform acquisition operations.

20. The method of claim 1, further comprising receiving authentication information from the user to verify the identity of the user.

21. The method of claim 20, wherein the authentication information comprises one of a digital certificate or a username and password.

22. The method of claim 1, further comprising:

receiving case information and target device information from a user to define a new inquiry;

creating a new inquiry based on the received information; and

associating the new inquiry with a case.

23. The method of claim 22, wherein the case information comprises at least one of a case number, case name, principle investigator, location to store the collected data, and a time zone for date/time reporting.

24. The method of claim 22, wherein the target computing device information includes at least one of a target computing device host name, IP address, operating system, access methods and password.

25. The method of claim 1, further comprising storing a copy of the computer evidence originally acquired from the target computing device.

26. The method of claim 1, further comprising:

normalizing the acquired computer evidence to a common format; and

storing the normalized computer evidence.

27. The method of claim 26, wherein normalizing the acquired computer evidence to a common format comprises at least one of converting timestamp data from a local time zone of the target computing device to a standard time zone, converting data having host names and IP addresses to all host names, converting data having host names and IP addresses to all IP addresses, and normalizing the clock of the target computing device to that of the forensic device.

28. The method of claim 1, further comprising:

performing a cryptographic hash on the computer evidence; and

storing the resulting hash value.

29. The method of claim 1, further comprising maintaining an audit log of transactions performed by the forensic device.

30. The method of claim 29, wherein maintaining the audit log comprises at least one of tracking computer evidence downloaded from the target computing device, browsing of the computer evidence by the remote user, and analyses performed on the computer evidence, and wherein the audit log comprises a timestamp corresponding to each transaction, an investigator identifier corresponding to the investigator performing each transaction, and a description of each transaction.

31. The method of claim 1, wherein the computer evidence comprises at least one log file, the method further comprising:

receiving input from the user to analyze the log file for tampering;

analyzing the log file to detect log file tampering; and

displaying to the user the results of the analysis.

32. The method of claim 31, wherein analyzing the log file to detect log file tampering comprises determining whether the entries in the log file are in ascending order.

33. The method of claim 31, wherein analyzing the log file to detect log file tampering comprises:

computing time gaps between entries of the log file;

identifying anomalous time gaps; and

displaying to the user the identified anomalous gaps.

34. The method of claim 31, wherein analyzing the log file to detect log file tampering comprises:

computing time gaps between entries of the log file;

generating a graphical representation of the time gaps; and

displaying the graphical representation to the user.

35. The method of claim 31, wherein analyzing the log file to detect log file tampering comprises:

receiving input that identifies a periodic event;

detecting an absent periodic event within the log file; and

alerting the user of the absent periodic events.

36. The method of claim 35, wherein receiving input that identifies the periodic event comprises:

receiving input that identifies a period of the periodic event; and

receiving input that identifies an identifier associated with the periodic event.

37. The method of claim 36, wherein detecting absent periodic events within the log file comprises:

searching for the log file for the periodic event identifier;

computing the amount of time that elapsed between each of the periodic event identifiers; and

comparing the period of the event with the computed elapsed times to detect absent periodic events.

38. The method of claim 35, wherein identifying the periodic event comprises receiving input from the user identifying the periodic event.

39. The method of claim 1, wherein acquiring the computer evidence from the target computing device comprises acquiring an image of at least one of a disk attached to the target computing device and a memory of the target computing device, and further comprising examining the acquired image to identify at least one of files, process or operating system

data structures, boot information, deleted files or directories, and data hidden in unallocated space.

40. The method of claim 1, wherein the communication link comprises a network.

41. The method of claim 1, wherein the communication link comprises one of a phone line, a universal serial bus (USB), a wireless port, a serial port, a parallel port and an infrared link.

42. The method of claim 1, wherein the target computing device comprises one of a personal computer, a handheld computer, a laptop, a workstation, a router, a gateway device, a firewall device, a web server, a file server, a database server, a mail server, a print server, a network-enabled personal digital assistant, and a network-enabled phone.

43. A system comprising:

a target computing device;

a forensic device coupled to the target computing device via a communication link;

a client device; and

a user interface module to present a user interface for the forensic device that is remotely accessible by the client device, wherein the forensic device receives input via the user interface that identifies computer evidence to acquire from a target computing device and, in response, acquires the computer evidence from the target computing device, stores the computer evidence, and presents the computer evidence to the remote user for analysis via the user interface.

44. The system of claim 43, wherein the forensic device presents the user interface to the remote user to allow the remote user to view and analyze the data on-line.

45. The system of claim 43, wherein the forensic device acquires additional computer evidence from the target computing device while the remote user views and analyzes the previously acquired computer evidence.

46. The system of claim 43, wherein the forensic device acquires the computer evidence from the target computing device while the target computing device is active.

47. The system of claim 43, wherein the forensic device acquires state information from the target computing device.

48. The system of claim 43, wherein the forensic device acquires the computer evidence from the target computing device without pre-loading acquisition software on the target computing device prior to acquiring the computer evidence.

49. The system of claim 43, wherein the forensic device receives input from the remote user that identifies at least one acquisition operation to perform, automatically selects at least one of a plurality of access methods via which to perform the acquisition operation based on the target computing device and type of computer evidence to acquire, and communicates commands associated with the acquisition operation to the target computing device to acquire corresponding computer evidence via the selected acquisition methods..

50. The system of claim 49, wherein the access methods include at least one of Windows Management Instrumentation (WMI), Server Message Block (SMB), Secure Shell (SSH), Remote Shell (RSH), Network File System (NFS), Apple Filing Protocol (AFP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP).

51. The system of claim 43, wherein the remote user identifies a plurality of acquisition operations to perform and the forensic device performs the acquisition operations in an order that reduces the impact on other data stored on the target computing device.

52. The system of claim 51, wherein the forensic device performs the acquisition operations to acquire at least one of a log file and communication statistics prior to any other acquisition operations.

53. The system of claim 52, wherein the forensic device performs an acquisition operation to acquire general system information from the target computing device after performing the acquisition operations to acquire the at least one of the log file and communication statistics prior to any other acquisition operations.

54. The system of claim 52, wherein the log file comprises one of a system event log, an application event log, a security event log, web server log file, Unix SYSLOG file, a mail log file, an accounting log file, and a router flow log file.

55. The system of claim 52, wherein the communications statistics comprises one of Ethernet statistics and network protocol statistics.

56. The system of claim 43, wherein the forensic device receives authentication information from the user to verify the identity of the user, the authentication information comprising one of a digital certificate or a username and password.

57. The system of claim 43, wherein the forensic device receives case information and target device information from a user to define a new inquiry, creates a new inquiry based on the received information, and associates the new inquiry with a case.

58. The system of claim 57, wherein the case information comprises at least one of a case number, case name, principle investigator, location to store the collected data, and a time zone for date/time reporting.

59. The system of claim 57, wherein the target computing device information includes at least one of a target computing device host name, IP address, operating system, access methods and password.

60. The system of claim 53, wherein the forensic device stores a copy of the computer evidence originally acquired from the target computing device, normalizes the acquired

computer evidence to a common format, stores the normalized computer evidence, performs a cryptographic hash on the computer evidence, and stores the resulting hash value.

61. The system of claim 43, wherein the forensic device maintains an audit log of transactions to track at least one of computer evidence downloaded from the target computing device, browsing of the computer evidence by the remote user, and analyses performed on the computer evidence, and wherein the audit log comprises a timestamp corresponding to each transaction, an investigator identifier corresponding to the investigator performing each transaction, and a description of each transaction.

62. The system of claim 53, wherein the computer evidence comprises at least one log file, and wherein the forensic device analyzes the log file to detect log file tampering and displays to the user the results of the analysis.

63. The system of claim 62, wherein the forensic device determines whether the entries in the log file are in ascending order.

64. The system of claim 62, wherein the forensic device computes time gaps between entries of the log file, identifies anomalous time gaps, and displays to the user the identified anomalous gaps.

65. The system of claim 62, wherein the forensic device computes time gaps between entries of the log file, generates a graphical representation of the time gaps, and displays the graphical representation to the user.

66. The system of claim 62, wherein the forensic device receives input identifying a period and an identifier associated with a periodic event, searches the log file for the periodic event identifier, computes the amount of time that elapsed between each of the periodic event identifiers, and compares the period of the event with the computed elapsed times to detect an absent periodic event, and alerts the user of the absent periodic event.

67. The system of claim 43, wherein the forensic device acquires an image of at least one of a disk attached to the target computing device and a memory of the target computing device and examines the acquired image to identify at least one of files, process or operating system data structures, boot information, deleted files or directories, and data hidden in unallocated space.

68. The system of claim 43, wherein the target computing device comprises one of a personal computer, a handheld computer, a laptop, a workstation, a router, a gateway device, a firewall device, a web server, a file server, a database server, a mail server, a print server, a network-enabled personal digital assistant, and a network-enabled phone.

69. The system of claim 43, wherein the communication link comprises a network.

70. The system of claim 43, wherein the communication link comprises one of a phone line, a universal serial bus (USB), a wireless port, a serial port, a parallel port and an infrared link.

71. An interrogation method to remotely acquire computer forensic evidence comprising:

receiving input from a remote user that identifies computer evidence to be acquired from a target computing device;

determining an order in which to perform acquisition operations to acquire the computer evidence from the target computing device with reduced impact on other data stored on the target computing device, wherein acquisition operations to acquire at least one of an log file and communication statistics occur in the order prior to any other acquisition operations; and

communicating commands to initiate the acquisition operations on the target computing device in accordance with the determined order.

72. The interrogation method of claim 71, wherein communicating commands associated with the acquisition operations to the target computing device comprises:

communicating commands associated with an acquisition operation to acquire at least one log file to the target computing device; and

communicating commands associated with an acquisition operation to acquire at least one set of communication statistics to the target computing device after the commands associated with the acquisition operation to acquire the log file.

73. The interrogation method of claim 72, further comprising communicating commands associated with an acquisition operation to acquire general system information to the target computing device after the commands associated with the acquisition operation to acquire the communication statistics.

74. The interrogation method of claim 71, wherein communicating commands associated with the acquisition operations to the target computing device comprises:

communicating commands associated with an acquisition operation to acquire communication statistics to the target computing device;

communicating commands associated with an acquisition operation to acquire log file to the target computing device after the commands associated with the acquisition operation to acquire the communication statistics.

75. The interrogation method of claim 74, further comprising communicating commands associated with an acquisition operation to acquire general system information to the target computing device after the commands associated with the acquisition operation to acquire the log file.

76. The interrogation method of claim 71, wherein the log comprises one of a system event log, an application event log, a security event log, web server log file, Unix SYSLOG file, a mail log file, an accounting log file, and a router flow log file.

77. The interrogation method of claim 71, wherein the communications statistics comprises one of Ethernet statistics and network protocol statistics.

78. A method comprising:

interrogating a target computing device to acquire a log file;

analyzing the log file to detect log file tampering; and

displaying to a user the results of the analysis.

79. The method of claim 78, wherein analyzing the log file to detect log file tampering comprises determining whether the entries in the log file are in ascending order.

80. The method of claim 78, wherein analyzing the log file to detect log file tampering comprises:

computing time gaps between entries of the log file;

identifying anomalous time gaps; and

displaying the identified anomalous time gaps to the user.

81. The method of claim 80, wherein identifying anomalous time gaps includes classifying the computed time gaps into bins of equal logarithmic size.

82. The method of claim 81, wherein classifying the computed time gaps into bins of equal logarithmic size includes classifying the computed time gaps into bins of equal logarithmic size in accordance with the equation $\text{Bin\#} = \text{floor}\left(\left(\left(\log\left(\text{gap}_i\right) - \log\left(\text{min}\right)\right)/\left(\log\left(\text{max}\right) - \log\left(\text{k}\right)\right)\right)*\text{bins}_{\text{max}}\right)$, wherein min is a dynamically calculated minimum gap size, max is a dynamically calculated maximum gap size, bins_{max} is a maximum number of bins, k is a minimum number of the smallest bin, and gap_i is an i^{th} gap size.

83. The method of claim 78, wherein analyzing the log file to detect log file tampering comprises:

computing time gaps between entries of the log file;

generating a graphical representation of the time gaps; and

displaying the graphical representation to the user.

84. The method of claim 78, wherein analyzing the log file to detect log file tampering comprises:

receiving input from the user that identifies a periodic event;

detecting an absent periodic event within the log file; and

alerting the user of the absent periodic event.

85. The method of claim 84, wherein identifying the periodic event comprises:

receiving input from the user that identifies a period of the periodic event; and

receiving input from the user that identifies an identifier of the periodic event.

86. The method of claim 85, wherein detecting the absent periodic event within the log file comprises:

searching for the log file for the periodic event identifier;

computing the time gap between each of the periodic event identifiers; and

comparing the period of the event with the computed time gaps to detect the absent periodic events.

87. An apparatus comprising:

an abstraction module that acquires data identified by a remote user from a target computing device and stores the computer evidence; and

a user interface module that presents the remote user with a user interface for the remote user to view and analyze the computer evidence.

88. The apparatus of claim 87, wherein the user interface module presents the user interface to the remote user to allow the remote user to view and analyze the data on-line.

89. The apparatus of claim 87, wherein the forensic device acquires additional computer evidence from the target computing device while the remote user views and analyzes the previously acquired computer evidence.

90. The apparatus of claim 87, wherein the abstraction module acquires the computer evidence from the target computing device while the target computing device is active.

91. The apparatus of claim 87, wherein the abstraction module acquires state information of the target computing device.

92. The apparatus of claim 87, wherein the abstraction module acquires the computer evidence from the target computing device without pre-loading acquisition software on the target computing device prior to acquiring the computer evidence.

93. The apparatus of claim 87, further comprising a data acquisition module that receives input from the remote user identifying at least one acquisition operation to perform and communicates the acquisition operations requested by the remote user to the abstraction module, which automatically selects at least one of a plurality of access methods via which to perform the acquisition operation based on the target computing device and type of computer evidence to acquire, and issues commands associated with the acquisition operation to the target computing device to acquire corresponding computer evidence via the selected acquisition methods..

94. The apparatus of claim 93, wherein the access methods include at least one of Windows Management Instrumentation (WMI), Server Message Block (SMB), Secure Shell (SSH), Remote Shell (RSH), Network File System (NFS), Apple Filing Protocol (AFP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP).

95. The apparatus of claim 87, wherein the remote user identifies a plurality of acquisition operations to perform and abstraction module performs the acquisition operations in an order that reduces the impact on other data stored on the target computing device.

96. The apparatus of claim 95, wherein the abstraction module performs the acquisition operations to acquire at least one of a log file and communication statistics prior to any other acquisition operations.

97. The apparatus of claim 87, wherein the apparatus receives case information and target device information from the remote user to define a new inquiry, creates a new inquiry based on the received information, and associates the new inquiry with a case.

98. The apparatus of claim 87, further comprising a data normalization module and a data preservation module, wherein the abstraction module stores a copy of the computer evidence originally acquired from the target computing device, the data normalization module normalizes the acquired computer evidence and stores the normalized computer evidence, and the data preservation module performs a cryptographic hash on the computer evidence and stores the resulting hash value.

99. The apparatus of claim 87, further comprising a tracking module that maintains an audit log of transactions to track at least one of computer evidence downloaded from the target computing device, browsing of the computer evidence by the remote user, and analyses performed on the computer evidence, and wherein the audit log comprises a timestamp corresponding to each transaction, an investigator identifier corresponding to the investigator performing each transaction, and a description of each transaction.

100. The apparatus of claim 87, further comprising a data analysis module that includes one or more analysis tools for viewing and analyzing the computer evidence, wherein the remote user may interact with the data analysis module to analyze an acquired log file to detect log file tampering.

101. The apparatus of claim 100, wherein the abstraction module acquires an image of at least one of a disk attached to the target computing device and a memory of the target computing device, and the data analysis module includes analysis tools for examining the acquired image to identify at least one of files, process or operating system data structures, boot information, deleted files or directories, and data hidden in unallocated space.

102. An apparatus comprising:

a data acquisition module that identifies one or more acquisition operations to perform to acquire computer evidence;

an abstraction module that performs the acquisition operations to acquire the computer evidence from a target computing device, wherein the abstraction module includes a plurality of interrogation agents that issue commands associated with the acquisition operations based on the type of operating system executed on the target computing device and the type of computer evidence desired;

a data analysis module that includes one or more data analysis tools; and

a user interface module to present a user interface for a remote user to interact with the data analysis module to view and analyze the collected computer evidence.

103. The apparatus of claim 102, wherein each of the interrogation agents is configured to communicate with a particular type of operating system and the analysis module selects one of the plurality of interrogation agents based on the type of operating system executed on the target computing device.

104. The apparatus of claim 102, wherein the interrogation agents use one of a plurality of access methods to acquire data from the target computing device.

105. The apparatus of claim 104, wherein the access methods include at least one of Windows Management Instrumentation (WMI), Server Message Block (SMB), Secure Shell (SSH), Remote Shell (RSH), Network File System (NFS), Apple Filing Protocol (AFP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP).

106. The apparatus of claim 102, wherein the computer evidence comprises at least one log file, and the remote user interacts with the data analysis module to analyze the log file to detect log file tampering.

107. The apparatus of claim 102, further comprising a data preservation module that performs a cryptographic hash on the computer evidence and stores the resulting hash value.

108. The apparatus of claim 107, wherein the data preservation module compares the resulting hash value with a hash value performed by the target computing device to ensure the integrity of the computer evidence in transit.

109. The apparatus of claim 102, further comprising a data normalization module to normalize the computer evidence to a common format to aid in analysis of the computer evidence.

110. A forensic analysis device that is adapted to operate as an intermediate device between a target computing device and a client device associated with a remote forensic investigator, wherein the analysis device comprises an acquisition module to acquire state information from the target computing device and store the state information on the forensic device while the target device remains active.

111. The forensic analysis device of claim 110, further comprising a user interface that allows the remote forensic investigator to view and analyze the previously acquired computer evidence on-line while the acquisition module acquires additional state information.

112. The forensic analysis device of claim 110, wherein the acquisition module acquires the computer evidence from the target computing device without pre-loading acquisition software on the target computing device prior to acquiring the computer evidence.

113. A computer-readable medium comprising instructions that cause a processor to:

receive input from a remote user of a client device that identifies computer evidence to acquire from a target computing device;

acquire the computer evidence from the target computing device with a forensic device coupled to the target computing device via a communication link;

store the computer evidence on the forensic device; and

present a user interface for the forensic device through which the remote user views and analyzes the computer evidence acquired from the target computing device.

114. The computer-readable medium of claim 113, wherein instructions to cause the processor to present the user interface for the forensic device include instruction to present the user interface for the forensic device through which the remote user views and analyzes the computer evidence acquired from the target computing device on-line.

115. The computer-readable medium of claim 113, further comprising instructions to cause the processor to acquire additional computer evidence while the remote user views and analyzes the previously acquired computer evidence.

116. The computer-readable medium of claim 113, wherein instructions to cause the processor to acquire the computer evidence from the target computing device includes instructions to cause the processor to acquire the computer evidence from the target computing device while the target computing device is active.

117. The computer-readable medium of claim 113, wherein instructions to cause the processor to acquire the computer evidence from the target computing device includes instructions to cause the processor to acquire state information from the target computing device.

118. The computer-readable medium of claim 113, wherein instructions to cause the processor to acquire the computer evidence from the target computing device includes acquire the computer evidence from the target computing device without pre-loading acquisition software on the target computing device prior to acquiring the computer evidence.

119. The computer-readable medium of claim 113, wherein instructions to cause the processor to receive input from the remote user that identifies computer evidence to acquire comprises instructions to cause the processor to receive input from the remote user that identifies at least one acquisition operation to perform, and further comprising instructions to cause the processor to:

automatically select at least one of a plurality of access methods via which to perform the acquisition operation based on the target computing device and the type of computer evidence to acquire; and

issue commands associated with the acquisition operation to the target computing device via the selected acquisition methods to acquire the computer evidence.

120. The computer-readable medium of claim 119, wherein instructions to cause the processor to issue commands associated with the acquisition operations comprises instructions to cause the processor to issue commands associated with the acquisition operations in an order that reduces the impact on other data stored on the target computing device.

121. The computer-readable medium of claim 113, further comprising instructions to cause the processor to:

store a copy of the computer evidence originally acquired from the target computing device;

normalize the acquired computer evidence to a common format;

store the normalized computer evidence;

perform a cryptographic hash on the computer evidence; and

store the resulting hash value.

122. The computer-readable medium of claim 113, further comprising instructions to cause the processor to maintain an audit log of transactions performed by the forensic device.